Proof: $\left\{ \frac{1}{\sqrt{N}} e_m \right\}_{m=0,\dots,N-1}$ is an orthonormal basis of $\ell^2(\mathbb{Z}(N))$, since the $\frac{1}{\sqrt{N}} e_m$ are orthogonal, normalised, and their number is equal to the dimension of $\ell^2(\mathbb{Z}(N))$. Since $a_m = (e_m, F)$, the result is clear. □

8.2 The fast Fourier transform

The "fast Fourier transform" is not a new definition of Fourier transform, it is an algorithm. It computes Fourier coefficients in a very economic way. It is rather simple, but clever, and it is worth studying as a great example of applied mathematics.

The context is as follows. We know $f \in L^2([0, 2\pi])$, and we want $\hat{f}$. Let us assume that f is smooth enough. For given N, let $F(r) = f(2\pi \frac{r}{N})$, $r = 0, \dots, N-1$. Then

$$a_k^N(F) = \frac{1}{N} \sum_{r=0}^{N-1} F(r)\, e^{-2\pi i \frac{kr}{N}}, \quad k = 0, \dots, N-1.$$

As $N \to \infty$ we get a Riemann integral, and

$$\lim_{N\to\infty} a_k^N(F) = \int_0^1 f(2\pi x)\, e^{-2\pi i k x}\, dx = \hat{f}(k).$$

The goal is to compute a_k^N for large N and all $k = 0, \dots, N-1$. The number of operations appears to be N^2, since each a_k^N requires N operations. The fast Fourier transform is much more efficient.

Theorem 8.3

If $N = 2^n$, one can calculate $\{a_k^N\}$ with less than $4 \cdot 2^n n = 4N \log_2 N = O(N \log N)$ operations.

The result is very surprising, since each a_k^N requires $O(N)$ operations!

Proof: The key idea is to proceed by induction. Having all numbers a_k^M, $k = 0, \dots, M-1$, we can use them to get a_k^{2M}, $k = 0, \dots, 2M-1$. Let

$$F_0(r) = F(2r)$$
$$F_1(r) = F(2r+1), \quad r = 0, \dots, M-1$$

We show that

$$a_k^{2M}(F) = \frac{1}{2}\left(a_k^M(F_0) + a_k^M(F_1)\, e^{-2\pi i \frac{k}{2M}} \right).$$

Indeed,

$$a_k^{2M}(F) = \frac{1}{2M} \sum_{r=0}^{2M-1} F(r)\, e^{-2\pi i \frac{kr}{2M}}$$
$$= \frac{1}{2}\Bigg(\underbrace{\frac{1}{M} \sum_{r=0}^{M-1} F(2r)\, e^{-2\pi i \frac{kr}{M}}}_{a_k^M(F_0)} + \underbrace{\frac{1}{M} \sum_{r=0}^{M-1} F(2r+1) e^{-2\pi i \frac{kr}{M}}}_{a_k^M(F_1)} e^{-2\pi i \frac{k}{2M}} \Bigg)$$

Let $K(M)$ denote the number of operations for a given function on $\mathbb{Z}(M)$. Because of the identity above, we have

$$K(2M) \leq 2K(M) + 8M.$$

The rest of the proof proceeds by induction. For $N = 2$, i.e. $n = 1$, we have $a_0^N(F) = \frac{1}{2}(F(0) + F(1))$, $a_1^N(F) = \frac{1}{2}(F(0) - F(1))$, and the bound is true. For $n+1$, we get (with $N = 2^n$)

$$K(2N) \leq 2K(N) + 8N \leq 8 \cdot 2^n n + 8 \cdot 2^n = 4 \cdot 2^{n+1}(n+1). \quad \square$$

8.3 Fourier theory of finite abelian groups

We now extend Fourier theory to arbitrary finite abelian groups. The situation is similar to $\mathbb{Z}(N)$, except that none of the explicit expressions is valid, and everything needs to be done from scratch.

Let $(G,\cdot)$ the finite abelian group and $\ell^2(G)$ the complex Hilbert space with inner product

$$(f,g) = \frac{1}{|G|} \sum_{a\in G} \overline{f(a)}\, g(a).$$

Definition: A character on G is a function $e : G \to \mathbb{C}$ such that

- $|e(a)| = 1 \quad \forall a \in G.$
- $e(a\cdot b) = e(a)\, e(b) \quad \forall a,b \in G.$

The dual group $\hat{G}$ of G is the set of characters of G.

Let us remark that $\hat{G} \neq 0$: it contains the function $G \to \{1\}$, the trivial character. The set $\hat{G}$ is itself an abelian group with the multiplication defined by

$$(e_1 \cdot e_2)(a) = e_1(a)\, e_2(a).$$

The trivial character is the unit element of $\hat{G}$.

Lemma 8.4

$$\sum_{a\in G} e(a) = 0$$

for every character e, except the trivial one.

Proof: Let $b \in G$ such that $e(b) \neq 1$. We have

$$e(b) \sum_{a\in G} e(a) = \sum_{a\in G} e(b\cdot a) = \sum_{a\in G} e(a).$$

(e is a character; the map $a \mapsto b\cdot a$ is a bijection)

The claim follows. □

Theorem 8.5

$\hat{G}$ is an orthonormal set.

Proof: $(e,e) = \frac{1}{|G|} \sum_{a\in G} |e(a)|^2 = 1.$

If $e \neq e'$, consider the function $f \in \ell^2(G)$ defined by

$$f(a) = (e(a))^{-1}\, e'(a).$$

It is easy to see that f is a (nontrivial) character. Since $(e(a))^{-1} = \overline{e(a)}$, we have by Lemma 8.4

$$0 = \sum_{a\in G} f(a) = \sum_{a\in G} \overline{e(a)}\, e'(a) = (e,e').$$

□

Since $\dim \ell^2(G) = |G|$, we see that $|\hat{G}| \leq |G|$. It is a remarkable fact that the characters actually form an orthonormal basis of $\ell^2(G)$, for all groups G. This is a special case of the Peter-Weyl theorem.

Theorem 8.6

$\hat{G}$ is an orthonormal basis of $\ell^2(G)$.

In order to prove Theorem 8.6 we need basic properties on the spectrum of matrices. Recall that complex matrices have an orthonormal basis of eigenvectors iff they are normal, i.e. iff $AA^* = A^*A$. This is the case of unitary matrices. Furthermore,

Lemma 8.7

Suppose that $T_1, \dots, T_k$ are normal matrices and that $T_i T_j = T_j T_i \ \forall i,j$. Then they can be diagonalised simultaneously, i.e. there exists an orthonormal basis $\{v_1, \dots, v_n\}$ such that v_i is eigenvector of all $T_1, \dots, T_k$.

Proof: By induction on k. This is clear for $k=1$. Assume that it holds for $k-1$, so that the vector space can be written as the direct sum

$$V_1 \oplus \dots \oplus V_\ell$$

where each V_i is characterised by the eigenvalues $(\lambda_1^{(i)}, \dots, \lambda_{k-1}^{(i)})$. We now check that each V_i is left invariant by T_k: If $v \in V_i$ is such that $T_j v = \lambda_j^{(i)} v \ \forall j = 1, \dots, k-1$, then

$$T_j T_k v = T_k T_j v = \lambda_j^{(i)} T_k v$$

for all $j = 1, \dots, k-1$, so that $T_k v \in V_i$. Then T_k is block-diagonal w.r.t. the direct sum above, and each block can be diagonalised separately. □

Proof of Theorem 8.6: We already know that the set of characters is orthonormal. We need to check that there are $|G|$ characters. Given $a \in G$, let

$$T_a : \ell^2(G) \to \ell^2(G)$$
$$(T_a f)(x) = f(a \cdot x), \quad x \in G.$$

(The notation "T" suggests "translation".) It is clear that T_a is linear, and

$$\|T_a f\|^2 = \sum_{x \in G} |f(a \cdot x)|^2 = \|f\|^2,$$

so T_a is unitary. Moreover, $T_a T_b = T_b T_a \ \forall a, b \in G$ (the group is abelian). Let $\{v_b\}_{b \in G}$ be an orthonormal basis of eigenvectors of all T_a's. We have

$$v_b(a) = v_b(a\cdot 1) = T_a v_b(1) \doteq \lambda_{ab}\, v_b(1).$$

Then $v_b(1) = 0$ implies that $v_b \equiv 0$, which is impossible. It follows that $v_b(1) \neq 0 \ \forall b \in G$.

Let us introduce $w_b(x) = \lambda_{xb} = \dfrac{v_b(x)}{v_b(1)}$. Then $|w_b(x)| = 1$ since T_x is unitary, and

$$w_b(x\cdot y) = \frac{v_b(x\cdot y)}{v_b(1)} = \frac{T_x\, v_b(y)}{v_b(1)} = \lambda_{xb}\,\frac{v_b(y)}{v_b(1)} = w_b(x)\, w_b(y).$$

Then w_b is a character. Finally,

$$(w_a, w_b) = \sum_{x\in G} \overline{w_a(x)}\, w_b(x) = \sum_{x\in G} \frac{\overline{v_a(x)}\, v_b(x)}{\overline{v_a(1)}\, v_b(1)} = 0$$

if $a \neq b$. We see that $\{w_a\}_{a\in G}$ is an orthonormal set with $|G|$ elements, so it is an orthonormal basis. □